PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification :	A2	(11) International Publication Number: WO 00/41535
Not classified		(43) International Publication Date: 20 July 2000 (20.07.00)

(21) International Application Number: PCT/US00/00701

(22) International Filing Date: 12 January 2000 (12.01.00)

(30) Priority Data:
60/115,835 14 January 1999 (14.01.99) US

(71) Applicant: LOCKSTAR, INC. [US/US]; 777 Passaic Avenuè, Clifton, NJ 07012 (US).

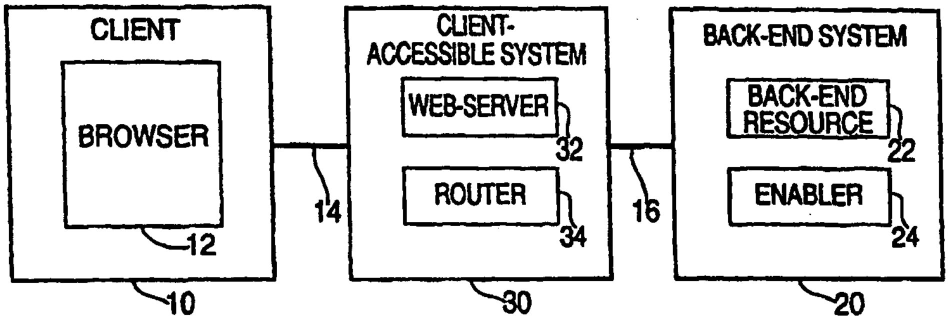
(72) Inventors: ORRIN, Steven, M.; 43 Conforti Avenue #77, West Orange, NJ 07052 (US). RUSSELL, James, P.; 27 Freeman Place, Nutley, NJ 07110 (US). GOLDBERG, Brian, D.; 1434 Pleasant Valley Way, West Orange, NJ 07052 (US). OLIK, Zbigniew, T.; 103 Lexington Avenue, Rocelle Park, NJ 07662 (US). OVITS, Mordechai; 113 Parkville Avenue, Brooklyn, NY 11230 (US). BENENSON, Paul; Apartment 3B, 127 Garden Street, Hoboken, NJ 07030 (US). MARCELLUS, Daniel, H.; 27 Cross Ridge Road, Tuxedo, NY 10987 (US). SCHNEIER, Bruce; 101 E. Minnehaha Parkway, Minneapolis, MN 55419-2680 (US). FERGUSON, Niels; Bart de Ligtstraat 64, NL-1097 JE Amsterdam (NL).

(74) Agent: MILLER, Joel; 17 Westwood Drive South, West Orange, NJ 07052-1822 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: SECURE DATA TRANSFER BETWEEN A CLIENT AND A BACK-END RESOURCE



(57) Abstract

Data can be securely passed between a client and a back-end resource by sending resource locators instead of the actual data. Using the protocol described here, the transfer of data is seamless, and prevents interception by any intermediate resource.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

SECURE DATA TRANSFER BETWEEN A CLIENT AND A BACK-END RESOURCE

Technical Field and Background Art

This application claims the benefit of U.S. Provisional Application no. 60/115,835 filed January 14, 1999.

In an on-line system, when data is retrieved from a remote resource, each intermediate point through which it travels may conceivably access the data. Even if such data is retrieved through a secure connection with a web server, the web server itself will be privy to the data. While the web server is beneficial in that it acts as intermediary between a client and a remote resource, it would be advantageous to utilize the services of the web server without having to compromise the data.

Brief Description of the Drawings

Figure 1 is a block diagram of a system affording secure data transfer; and

Figures 2 and 3 are flow charts of the operation of the system of Figure 1.

Modes for Carrying Out the Invention

Secure transfer of data between a client and back-end resources over the Internet can be achieved in part by establishing a secure path between the two points. Formatting and protocol issues not requiring access to secure data can be delegated to conventional elements in the path.

In one configuration, illustrated in the block diagram of Figure 1, a client 10, using an Internet browser 12 equipped with the means necessary to create a secure session, accesses a back-end system 20 on which a back-end resource 22 resides, through a client-accessible system 30. The back-end resource 22 may be a database or some other source of data or device that the client wishes to access.

The interconnection 14 between the client 10 and the client-accessible system 30 can be over a network such as the Internet or through some other medium. Similarly, the interconnection 16 between the client-accessible system 30 and the back-end system 20 can be over a network such as the Internet or through some other data link.

The data transfer process can be described in two parts: a download procedure (Figure 2), where data is transferred from the back-end resource to the client, and an upload procedure (Figure 3), where data travels from the client to the back-end resource. Either can be used alone, in concert with each other, or with other processes as appropriate.

Download Procedure

As shown in Figure 2, the client 10 can initiate a download of information by sending a request to the web server 32, which passes the request on to the enabler 24. In response to the request, the enabler 24 issues one or more resource locators and passes them to the web server 32. Typically, these resource locators are addresses that point to data resources on the back end system 20. The web server 32 treats the resource locators it receives from the enabler 24 as data.

The web server 32 assembles a web page placing the resource locators in the web page where it would otherwise insert data. It then sends the formatted web page to the browser 12 at the client 10.

As the web page loads in the browser 12, the resource locators cause the browser 12 to access the back-end system through a router 34 on the client-accessible system 30. After optionally authenticating the client 10, the enabler 24 will send the browser 12 the appropriate data in response to the resource locator, and the browser 12 will simply insert each datum in the formatted page at the location dictated by the physical location of each resource locator on the page. The path between the browser 12 and the enabler 24 through the router 34 is secure, having invoked a secure protocol such as SSL ("secure socket layer").

The data has thus been sent from the back-end resource 20 to the browser 12 via a path secure with respect to the elements of the client-accessible system 30 and interconnections 14 and 16, i.e., bypassing the web server 32.

Upload Procedure

In an upload, as shown in Figure 3, the client 10 desires to send data to the back-end resource 22, but in a manner in which the data is not accessible or readable by the client-accessible system 30 or interconnections 14 and 16. To do so, the client 10 establishes a secure session with the enabler 24 through the router 34, optionally insuring authentication of the back-end system 20 and/or the client 10. The client 10 then sends the data to the enabler 24 over the secure path.

The enabler 24 does not have a service request and as such cannot utilize the data at this point. Therefore, the data is stored on the back-end system 20 for later retrieval and, in response to the original message, the enabler 24 issues a redirect command and a resource locator and passes them back to the client 10 through the router 34. This may occur through a secure path. For example, the redirect can assume the form: https://ws:443/arg:xyz, where ws:443 designates the secure port 443 on the web server 32 and "xyz" is the resource locator that the web server 32 will use when referring to the data earlier passed to the enabler 24.

The client 10 now executes the redirect command, establishing a session with the web server 32. As part of executing the redirect command, the client 10 sends the resource locator to the web server 32. Again, this can be done over a secure path. The web server 32 in turn generates a service request for the back-end system 20, using the resource locator in lieu of the actual data, and passes this to the enabler 24 on the back-end system 20. When the enabler 24 receives the resource locator, the enabler 24 will fetch the data corresponding to the resource locator and associate it with the service request.

As required previously, authentication can be performed using any method including the method described in provisional patent application No. 60/106,290, titled "Secure Authentication for Access to Back-End Resources," and filed October 30, 1998, incorporated by reference herein.

What is claimed is:

1. A method for downloading data from a back-end resource to a client via network-based client-accessible systems containing web servers, comprising the steps of:

sending a client-originated request from the client to the back-end resource via a client-accessible system;

issuing at least one back-end resource locator and passing it to a web server;

formatting a web page with the resource locators and passing it to the client; and

reading the web page and retrieving the data over secure connections according to the resource locators.

2. A method as set forth in claim 1, where the step of retrieving the data over secure connections according to the resource locators comprises the step of bypassing the web server.

3. A method as set forth in claim 1, where the step of requesting retrieval of the data comprises the step of authenticating the client.

4. A method for uploading data from a client to a back-end resource via network-based client-accessible systems containing web servers, comprising the steps of:

establishing a secure session between the client and the back-end resource via a client-accessible system;

sending data from the client to the back-end resource via the secure path;

issuing a redirect command and a resource locator, and passing them from the back-end resource to the client;

executing the redirect command and establishing a session between the client and the web-server;

sending the resource locator from the client to the web-server;

sending the resource locator from the web-server to the back-end resource; and

locating the data at the back-end resource using the resource locator.

5. A method as set forth in claim 4, where the step of sending data from the client to the back-end resource via the secure path comprises the step of bypassing the web server.

6. A method as set forth in claim 4, where the step of establishing a secure session between the client and the back-end resource via a client-accessible system comprises the step of authenticating the back-end resource and/or the client.

7. A system for downloading data from a back-end resource to a client via network-based client-accessible systems containing web servers, comprising:

a back-end system comprising

a back-end resource; and

an enabler, the enabler comprising means for generating at least one resource locator, the resource locator comprising a redirect command corresponding to the back-end resource; and

at least one network-based client-accessible system comprising

at least one web-server, the web-server comprising

means for assembling a web page; and

means for incorporating a resource locator in the web page; and

a router comprising

at least one port corresponding to a redirect command in a resource locator;

means for establishing a secure path with the client; and

means for communicating with the back-end resource.

8. A system as set forth in claim 7, where the enabler further comprises means for authenticating the client.

9. A system for uploading data from a client to a back-end resource via network-based client-accessible systems containing web servers, comprising:

a back-end system comprising

a back-end resource; and

an enabler, the enabler comprising means for generating at least one resource locator, the resource locator comprising a redirect command corresponding to the back-end resource; and

at least one network-based client-accessible system comprising at least one web-server, the web-server comprising means for communicating with the client and the back-end system; and

a router comprising means for providing a secure connection between the client and the back-end system.

10. A system as set forth in claim 9, further comprising means for authenticating the client.

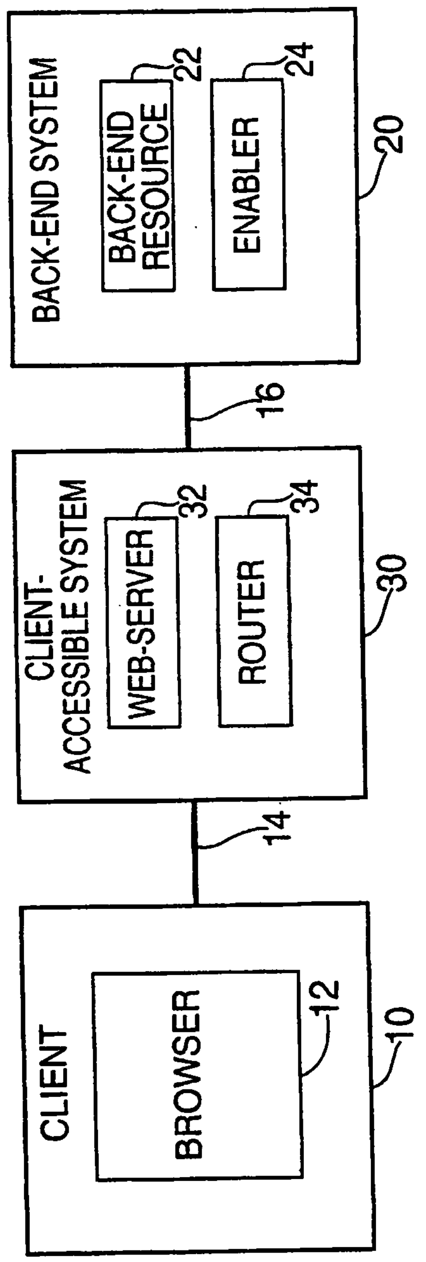

BACK-END SYSTEM
BACK-END RESOURCE
22
ENABLER
24
20
16
CLIENT-ACCESSIBLE SYSTEM
WEB-SERVER
32
ROUTER
34
30
14
CLIENT
BROWSER
12
10

FIG. 1

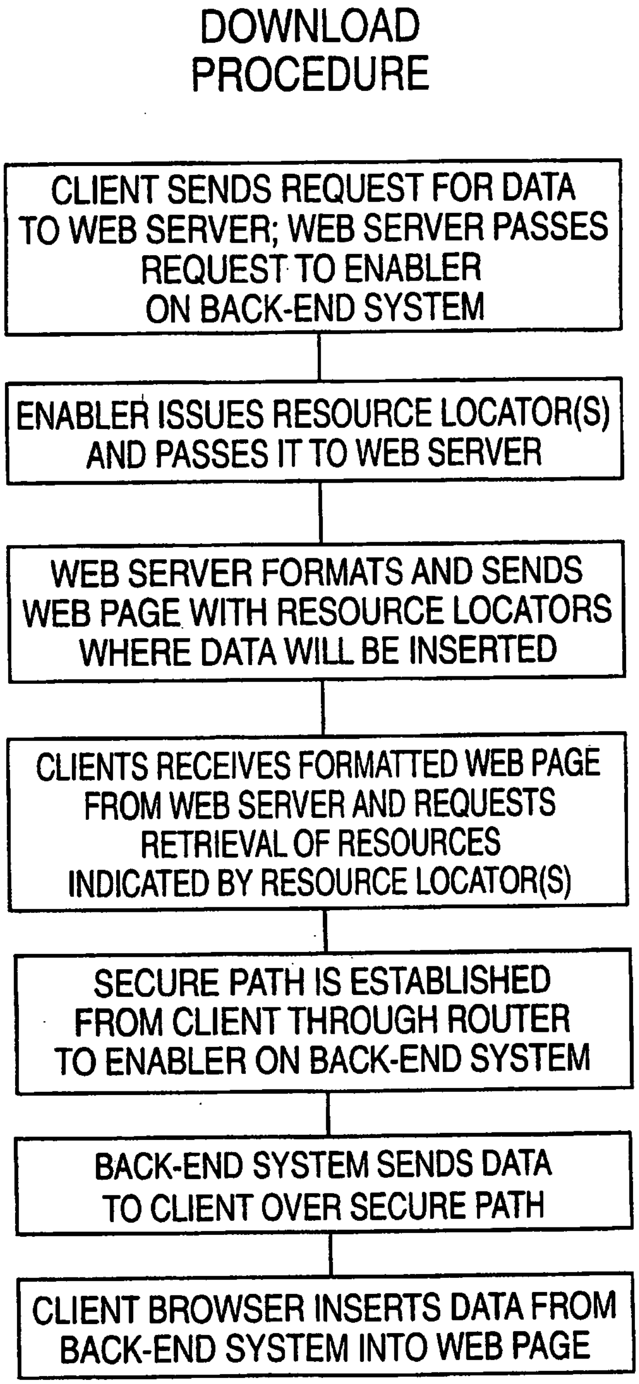

DOWNLOAD
PROCEDURE
CLIENT SENDS REQUEST FOR DATA TO WEB SERVER; WEB SERVER PASSES REQUEST TO ENABLER ON BACK-END SYSTEM
ENABLER ISSUES RESOURCE LOCATOR(S) AND PASSES IT TO WEB SERVER
WEB SERVER FORMATS AND SENDS WEB PAGE WITH RESOURCE LOCATORS WHERE DATA WILL BE INSERTED
CLIENTS RECEIVES FORMATTED WEB PAGE FROM WEB SERVER AND REQUESTS RETRIEVAL OF RESOURCES INDICATED BY RESOURCE LOCATOR(S)
SECURE PATH IS ESTABLISHED FROM CLIENT THROUGH ROUTER TO ENABLER ON BACK-END SYSTEM
BACK-END SYSTEM SENDS DATA TO CLIENT OVER SECURE PATH
CLIENT BROWSER INSERTS DATA FROM BACK-END SYSTEM INTO WEB PAGE

FIG. 2

UPLOAD
PROCEDURE

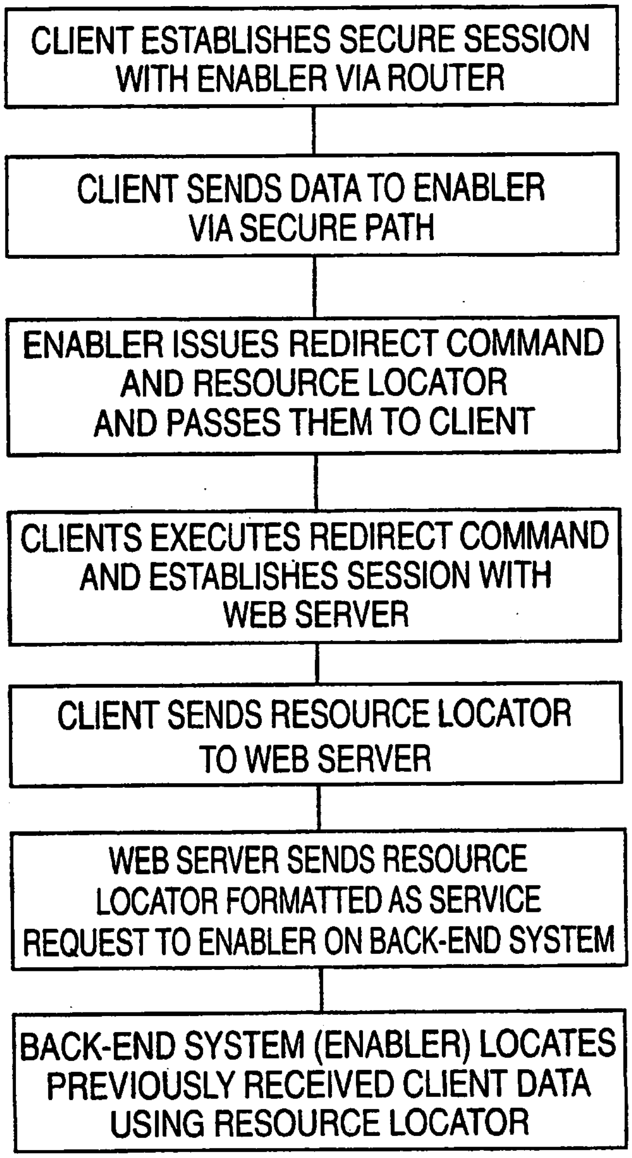

CLIENT ESTABLISHES SECURE SESSION WITH ENABLER VIA ROUTER
CLIENT SENDS DATA TO ENABLER VIA SECURE PATH
ENABLER ISSUES REDIRECT COMMAND AND RESOURCE LOCATOR AND PASSES THEM TO CLIENT
CLIENTS EXECUTES REDIRECT COMMAND AND ESTABLISHES SESSION WITH WEB SERVER
CLIENT SENDS RESOURCE LOCATOR TO WEB SERVER
WEB SERVER SENDS RESOURCE LOCATOR FORMATTED AS SERVICE REQUEST TO ENABLER ON BACK-END SYSTEM
BACK-END SYSTEM (ENABLER) LOCATES PREVIOUSLY RECEIVED CLIENT DATA USING RESOURCE LOCATOR

FIG. 3

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7:
H04L 29/06

A3

(11) International Publication Number: WO 00/41535

(43) International Publication Date: 20 July 2000 (20.07.00)

(21) International Application Number: PCT/US00/00701

(22) International Filing Date: 12 January 2000 (12.01.00)

(30) Priority Data:
60/115,835 14 January 1999 (14.01.99) US

(71) Applicant: LOCKSTAR, INC. [US/US]; 777 Passaic Avenue, Clifton, NJ 07012 (US).

(72) Inventors: ORRIN, Steven, M.; 43 Conforti Avenue #77, West Orange, NJ 07052 (US). RUSSELL, James, P.; 27 Freeman Place, Nutley, NJ 07110 (US). GOLDBERG, Brian, D.; 1434 Pleasant Valley Way, West Orange, NJ 07052 (US). OLIK, Zbigniew, T.; 103 Lexington Avenue, Rocelle Park, NJ 07662 (US). OVITS, Mordechai; 113 Parkville Avenue, Brooklyn, NY 11230 (US). BENENSON, Paul; Apartment 3B, 127 Garden Street, Hoboken, NJ 07030 (US). MARCELLUS, Daniel, H.; 27 Cross Ridge Road, Tuxedo, NY 10987 (US). SCHNEIER, Bruce; 101 E. Minnehaha Parkway, Minneapolis, MN 55419-2680 (US). FERGUSON, Niels; Bart de Ligtstraat 64, NL-1097 JE Amsterdam (NL).

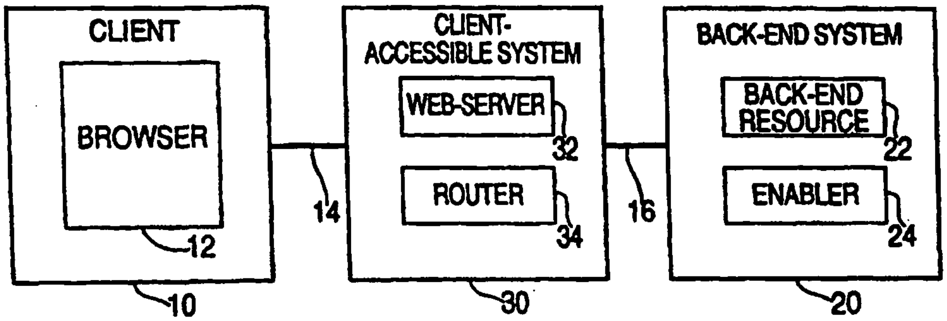
(74) Agent: MILLER, Joel; 17 Westwood Drive South, West Orange, NJ 07052-1822 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(88) Date of publication of the international search report:
2 November 2000 (02.11.00)

(54) Title: SECURE DATA TRANSFER



(57) Abstract

Data can be securely passed between a client and a back-end resource by sending resource locators instead of the actual data. Using the protocol described here, the transfer of data is seamless, and prevents interception by any intermediate resource.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

INTERNATIONAL SEARCH REPORT

Intern. al Application No
PCT/US 00/00701

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 814 589 A (AT & T CORP) 29 December 1997 (1997-12-29) page 3, line 19 -page 4, line 18 abstract figure 3 ---	1-10
X	WO 98 58332 A (ERICSSON TELEFON AB L M) 23 December 1998 (1998-12-23) abstract --- -/--	1-10

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 9 August 2000	Date of mailing of the international search report 17/08/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Canosa Aresté, C

INTERNATIONAL SEARCH REPORT

Interr ıal Application No
PCT/US 00/00701

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	KOLLETZKI S: "Secure Internet banking with Privacy Enhanced Mail -- A protocol for reliable exchange of secured order forms" COMPUTER NETWORKS AND ISDN SYSTEMS,NL,NORTH HOLLAND PUBLISHING. AMSTERDAM, vol. 28, no. 14, 1 November 1996 (1996-11-01), pages 1891-1899, XP004014500 ISSN: 0169-7552 page 1896 -----	1-10

INTERNATIONAL SEARCH REPORT

..ormation on patent family members

Intern ıal Application No
PCT/US 00/00701

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
EP 0814589	A	29-12-1997	US	6058250	A	02-05-2000
			CA	2204058	A	19-12-1997
WO 9858332	A	23-12-1998	AU	8050298	A	04-01-1999